UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,982	08/29/2001	Takashi Endo	NIT-295	5993

24956 7590 01/28/2008

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
01/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/940,982	ENDO ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 18-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8 and 18-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20070606, 20070815*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A petition was received on 07 March 2007, such petition requesting entry and consideration of the supplemental response received 24 November 2006. The petition was dismissed as of 10 July 2007. A request for reconsideration of the decision was received on 20 July 2007. The re-filed petition was denied as of 20 November 2007.

2. A response was received concurrently with the request for reconsideration on 20 July 2007. By this response, new Claims 18-22 have been added. No claims have been amended or canceled. Claims 1-8 and 18-22 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments filed 20 July 2007 have been fully considered but they are not persuasive.

Claims 1-8 were rejected under 35 U.S.C. 103(a) as unpatentable over applicant admitted prior art in view of Jaffe et al, US Patent 6510518.

Regarding independent Claim 1, Applicant first summarizes and substantially repeats arguments presented in the response received 08 November 2006 (see pages 8-9 of the present response; see also pages 8-9 of the response received 08 November 2006). The Examiner previously responded to these arguments, noting that the assertions amounted to broad supposition or allegation by Applicant of what would

result from the combination of the admitted prior art and the teachings of Jaffe (quoted from the previous action in the present response at pages 9-10). In response, Applicant asserts that Applicant's proposals "are an attempt to focus the issue of just what the allegedly combinable teachings of the references would have suggested to [one of] ordinary skill in the art" (page 10 of the present response, emphasis in original) and alleges that "the rejection does not explain, except to use the claim as a roadmap, what the result of modifying the admitted prior art according to Jaffe would be" and requests "the Examiner to indicate the result of combining Jaffe with the admitted prior art, using those teachings, rather than the claim, as a roadmap" (page 10 of the present response). The Examiner disagrees with the above allegation but will gladly comply with the above request.

Specifically, as the Examiner believes was previously clearly set forth, Jaffe broadly teaches that data used in cryptographic processing can be represented using a constant Hamming weight representation (Jaffe, column 4, line 55-column 5, line 30, as previously cited). The admitted prior art disclosed every structural limitation of the apparatus of Claim 1, which Applicant has not disputed, but was silent as to the use of constant Hamming weight disturbance data. Jaffe discloses that one would be motivated to use the above-noted constant Hamming weight data representation for data used in cryptographic processing (such as the data within the admitted prior art apparatus) in order to minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48, as previously cited). Even more explicitly, Jaffe discloses that the invention disclose therein "transforms the basic

representation of data" and that a "constant Hamming weight data representation replaces conventional bit representations commonly employed in the background art" (Jaffe, column 2, lines 56-60). This is a clear disclosure (or, to use Applicant's term, roadmap) that the constant Hamming weight representation taught by Jaffe is intended to be used for ALL data in a system, which, when applied to the teachings of the admitted prior art apparatus, clearly would include representing the disturbance data, as taught by the admitted prior art, using the constant Hamming weight representation.

The Examiner again notes that Applicant has not provided any evidence, such as citations to the prior art or elsewhere, in support of the arguments (see pages 8-11 of the present response). Although Applicant alleges that there is no evidence to be shown because the prior art does not suggest the combination (page 10 of the present response), the Examiner notes that Applicant has not provided any evidence of what Applicant does consider the prior art to teach or suggest. For example, although Applicant refers repeatedly to a mapping operation taught by Jaffe (pages 8-10 of the present response), Applicant has not provided any evidence in support of this interpretation. The Examiner reiterates that Jaffe does not suggest "mapping" as a specific operation to be performed as part of processing, but rather as a type of representation of the binary values of TRUE and FALSE (see the general description of various representations at Jaffe, column 4, line 55-column 5, line 30).

Applicant finally "reasserts their prior arguments that Jaffe does not contain teachings so broad as to suggest to one of ordinary skill to use a constant hamming weight representation for all data within a system" (see page 11 of the present

response; see also pages 8-9 of the response filed 16 October 2006, and the summary of the interview conducted on 12 September 2006). However, as detailed above, the Examiner again asserts that Jaffe does, in fact, teach precisely that (see Jaffe, column 2, lines 56-60; see also the summary of the interview conducted 12 September 2006, the advisory action mailed 30 October 2006, and page 4 of the Office action mailed 20 February 2007).

Regarding dependent Claims 2-8, Applicants refer back to "all arguments previously presented". In response, the Examiner notes that a detailed response to each of the arguments regarding the dependent Claims (such as those at pages 11-15 of the response received 16 October 2006) was set forth in the Office action mailed 20 February 2007 (see pages 5-7 of that action). The Examiner notes that Applicant has not attempted to rebut the Examiner's responses.

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Regarding new Claims 18-22, Applicant argues that "no document of record recognizes the value of first disturbance data having a constant hamming weight" (page 11 of the present response). However, as noted above, Jaffe provides a clear teaching for a constant Hamming weight representation of all data in a system (see Jaffe, column 4, line 55-column 5, line 30, and column 2, lines 56-60). Similarly, Applicant argues that the references do not address the concatenation of m-bit random number randomly into an n-bit random number (page 12 of the present response); however, the Examiner believes that this limitation corresponds substantially to the limitations of dependent

Claims 7 and 8, which are found to have support at least in Jaffe, as previously described.

Further regarding the new Claims, Applicant provides additional arguments with respect to dependent Claims 19-22 (see page 13 of the present response). These arguments, along with any arguments regarding independent Claim 18 that have not been explicitly addressed above, are addressed by the new grounds of rejection of the new claims, set forth below.

4. The Examiner notes that Applicant's remarks include references to "Preliminary Amendments" dated 08 November 2006 and 24 November 2006 (see page 8 of the present response). However, the Examiner notes that neither of these responses were, in fact, preliminary amendments as defined in 37 CFR 1.115(a), which defines a preliminary amendment as "an amendment that is received in the Office (§ 1.6) on or before the mail date of the first Office action under § 1.104". Both of the above responses (received 08 and 24 November 2006) were received after Office actions mailed 15 June 2005, 03 October 2005, and 08 May 2006, and are clearly not preliminary amendments as defined in 37 CFR 1.115(a).

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 18-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 18 recites the limitation "the predetermined number of the m-bit random numbers" in lines 6-7 of the claim. There is insufficient antecedent basis for this limitation in the claim. It is also noted that although the claim recites that the processor generates second disturbance data (lines 8-9 and 14) and evaluates whether the second disturbance data has a target Hamming weight (lines 9-10), there is no other processing for which the second disturbance data is used, and there is also nowhere that the result of the evaluation is used.

Claim 21 recites the limitation "the transform operation" in line 4. There is insufficient antecedent basis for this limitation in the claims.

Claims 19, 20, and 22 are rejected due to their dependence on rejected Claim 18.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-8 and 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Jaffe et al, US Patent 6510518.

In reference to Claim 1, Applicant admits as prior art an apparatus including a data transform means transforming input data by using disturbance data to generate transformed data, a transformed data processing means for carrying out predetermined processing on the transformed data to generate processed transformed data, and a data inverse transform means for carrying out inverse transformation processing on the processed transformed data using processed disturbance data to generate processed data (see page 21, lines 1-12 of the present application). However, Applicant admits that such prior art does not explicitly disclose that the disturbance data and the processed disturbance data have a constant Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30; see also column 2, lines 56-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

In reference to Claim 2, Applicant admits that the prior art further discloses that the processed disturbance data can be generated by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application; see also prior art Figure 4).

In reference to Claim 3, Jaffe further discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45, and column 5, lines 12-18).

In reference to Claim 4, Applicant admits that the prior art further discloses generating processed disturbance data by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application; see also prior art Figure 4, and Jaffe, column 4, line 55-column 5, line 30).

In reference to Claim 5, Applicant further admits and Jaffe further discloses a disturbance data storage means, disturbance data select means, and that processing is carried out on the disturbance data in order to generate the processed disturbance data (page 21, lines 6-8 of the present application, and prior art Figure 4; Jaffe, column 16, lines 15-32).

In reference to Claim 6, Jaffe further discloses means for generating random numbers each having a Hamming weight equal to half the numbers of bits include in the random number (column 7, lines 62-64; see Figures 1 and 4; see also column 5, lines 12-18), means for inverting bits of data (column 8, lines 41-45; Figure1, step 150; Figure 4, step 450), and means for concatenating a random number with data output by the means for inverting (Figure 1, steps 110-120; Figure 4, steps 410-420).

In reference to Claim 7, Jaffe further discloses a random number generation means (column 7, lines 62-64), a Hamming weight computation means (see Figure 1; column 8, lines 25-29 and 46-65), a Hamming weight examination means (see Figure 1; column 8, lines 25-29 and 46-65), and a constant Hamming weight assurance means

(see column 4, line 55-column 5, line 30, where the representations guarantee a constant Hamming weight).

In reference to Claim 8, Jaffe further discloses random number generation means to generate partial random numbers with uniform constant Hamming weights and bit count each equal to a fraction of a final random number (Figure 1, step 115; Figure 4, step 415); means to generate random numbers until a sum of bit counts is equal to the final bit count (column 7, lines 62-64); and means for concatenating the partial random numbers (Figure 1, steps 110-120; Figure 4, steps 410-420).

In reference to Claim 18, Applicant admits as prior art an apparatus including a processor (see prior art Figure 2, CPU 201, coprocessor 202; page 2, line 14-page 3, line 5 of the present application), a storage (Figure 2, storage device 204; page 2, lines 14-17; page 3, line 8–page 4, line 2) arranged to store programs (Figure 2, program memory 205; page 3, line 12) and data (Figure 2, data memory 206; page 3, lines 12-14), and a data bus interconnecting the processor and storage (Figure 2, bus 203; page 3, lines 5-7). Applicant further admits that the processor is arranged to transform input data into first transformed data with first disturbance data, process the first transformed data with a first operation, generate second transformed data, process the first disturbance data with the first operation, generate second disturbance data, and inverse-transform the second transformed data into processed data (see page 21, lines 1-12 of the present application). However, Applicant admits that such prior art does not explicitly disclose that the second disturbance data have a target Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30; see also column 2, lines 56-60). Jaffe further discloses a processor arranged to generate m-bit random numbers having a predetermined Hamming weight (column 7, lines 62-64; Figure 1, step 115; Figure 4, step 415), concatenate m-bit random numbers randomly into data of n bits equal to a multiple of m (column 7, lines 62-64; Figure 1, steps 110-120; Figure 4, steps 410-420), and evaluate whether data has a target Hamming weight (see Figure 1; column 8, lines 25-29 and 46-65; see column 4, line 55-column 5, line 30; where the representations guarantee a constant Hamming weight). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

In reference to Claim 19, Jaffe further discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45, and column 5, lines 12-18).

In reference to Claim 20, Jaffe further discloses collecting m-bit random numbers in a table (see column 15, line 60-column 16, line 14; column 7, lines 62-64; Figure 1, step 115; Figure 4, step 415).

In reference to Claim 21, Applicant further admits and Jaffe further discloses transforming data by means of an XOR operation (or an addition or transform operation) (see pages 8 and 9 of the present application, noting Expressions 3, 4, 5, 7, 9, and 10,

in particular; see also Jaffe, Figures 1-4 in general, also noting column 2, line 60-column 3, line 20, for example).

In reference to Claim 22, Applicant further admits and Jaffe further discloses performing a rotate operation, a shift operation, or a bit permutation operation (see pages 8 and 9 of the present application, noting Expressions 2, 6, and 8 in particular; see also Jaffe, Figures 1-4 in general, also noting column 11, line 61-column 12, line 19, for example).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Chow et al, WIPO Publication WO01/61916, was included with the information disclosure statement received 06 June 2007, and appears on the European search report included with that information disclosure statement, but was not cited on the information disclosure statement.

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/23/08